

**AMENDMENT TO**  
**RULES COMMITTEE PRINT 118–10**  
**OFFERED BY MR. GIMENEZ OF FLORIDA**

At the end of subtitle C of title XV, insert the following new section:

**1 SEC. 15\_\_\_\_. PORT INFRASTRUCTURE CYBERSECURITY RE-**  
**2 VIEW.**

**3 (a) REVIEW.**—Not later than 240 days after the date  
**4 of the enactment of this Act, the Secretary of Homeland**  
**5 Security, acting through the Commandant of the United**  
**6 States Coast Guard, in coordination with the Director of**  
**7 the Cybersecurity and Infrastructure Security Agency,**  
**8 shall—**

**9 (1) conduct a security risk assessment to im-**  
**10 prove the cybersecurity of each information and**  
**11 operational technology system used or operated by**  
**12 each covered strategic seaport; and**

**13 (2) develop recommendations to address any**  
**14 risks identified.**

**15 (b) ELEMENTS.**—The security risk assessment under  
**16 subsection (a)(1) shall include, with respect to each cov-**  
**17 ered strategic seaport, the following:**

1           (1) An assessment of any risks or threats posed  
2       by cybersecurity vulnerabilities of the information  
3       and operational technology systems used or operated  
4       by each covered strategic seaport, including all cov-  
5       ered port infrastructure equipment that is manufac-  
6       tured, controlled or designed by a covered foreign  
7       adversary or a covered foreign entity.

8           (2) An assessment of whether there are any  
9       other vulnerabilities in the information and oper-  
10      ational technology systems used or operated by each  
11      covered strategic seaport or covered port infrastruc-  
12      ture equipment.

13          (3) An assessment of necessary improvements  
14      to such systems or equipment that would be needed  
15      to meet, directly or indirectly, national security and  
16      defense readiness requirements.

17      (c) CONSULTATION.—The Secretary of Homeland Se-  
18      curity shall conduct the security risk assessment under  
19      subsection (a)(1) and develop the report under subsection  
20      (d) in consultation with the Secretary of Defense, the Sec-  
21      retary of Transportation, and the Area Maritime Security  
22      Advisory Committees established under section 70112(b)  
23      of title 46, United States Code.

24      (d) REPORT TO CONGRESS.—

1           (1) REPORT.—Not later than one year after the  
2           date of the enactment of this Act, the Secretary of  
3           Homeland Security, in coordination with the Sec-  
4           retary of Defense, shall submit to the appropriate  
5           congressional committees a report containing—

6                   (A) a list of tools, techniques, and proce-  
7                   dures used to test each electronic system;

8                   (B) a list of maritime and transportation  
9                   operational technologies examined;

10                  (C) a list of stakeholders involved in the  
11                  assessments;

12                  (D) critical and high-risk cybersecurity  
13                  vulnerabilities posed by existing or newly con-  
14                  structed ship-to-shore cranes manufactured, in  
15                  whole or in part, by a covered foreign adversary  
16                  or a covered foreign entity that is in use at  
17                  United States covered strategic seaports;

18                  (E) critical and high-risk cybersecurity  
19                  vulnerabilities posed by existing or newly pur-  
20                  chased software, hardware, or cloud architec-  
21                  ture designed or manufactured in whole or in  
22                  part by a covered foreign adversary or a cov-  
23                  ered foreign entity that is in use at each cov-  
24                  ered strategic seaport;

1 (F) a prioritized list of cybersecurity  
2 vulnerabilities discovered in each covered stra-  
3 tegic seaport that are essential for mobilization  
4 or contingency responses of the Armed Forces,  
5 including Military Ocean Terminals;

6 (G) a description of any gaps in authority  
7 or jurisdiction at the intersection of United  
8 States military property and civilian critical in-  
9 frastructure; and

10 (H) risk-prioritized recommendations to  
11 mitigate threats to the defense readiness, na-  
12 tional security, and continuity of the economy  
13 of the United States through enhanced cyberse-  
14 curity at each covered strategic seaport and  
15 surrounding critical infrastructure.

16 (2) FORM.—The report required under para-  
17 graph (1) shall be submitted in unclassified form,  
18 but may include a classified annex.

19 (e) PROHIBITION.—Notwithstanding any other provi-  
20 sion of law, no covered port infrastructure equipment for  
21 which a contract is entered into after the date that is five  
22 years after the date of the enactment of this Act, may  
23 be operated at any covered strategic seaport.

24 (f) DEFINITIONS.—In this section:

1           (1) The term “appropriate congressional com-  
2       mittees” means—

3           (A) the Committee on Homeland Security,  
4       the Committee on Transportation and Infra-  
5       structure, the Committee on Armed Services,  
6       and the Select Committee on the Strategic  
7       Competition Between the United States and the  
8       Chinese Communist Party of the House of Rep-  
9       resentatives; and

10          (B) the Committee on Homeland Security  
11       and Governmental Affairs, the Committee on  
12       Commerce, Science, and Transportation, and  
13       the Committee on Armed Services of the Sen-  
14       ate.

15          (2) The term “continuity of the economy”  
16       means the distribution of goods and services across  
17       the United States necessary for the reliable func-  
18       tioning of the United States economy during a sig-  
19       nificant event, through key channels of interstate  
20       commerce, including—

21           (A) bulk power and electric transmission  
22       systems;

23           (B) national and international financial  
24       systems, including wholesale payments, stocks,  
25       and currency exchanges;

1 (C) national and international communica-  
2 tions networks, data-hosting services, and cloud  
3 services;

4 (D) interstate oil and natural gas pipe-  
5 lines; and

6 (E) mechanisms for the interstate and  
7 international trade and distribution of mate-  
8 rials, food, and medical supplies, including  
9 road, rail, air, and maritime shipping.

10 (3) The term “covered foreign adversary”  
11 means—

12 (A) any foreign government or other for-  
13 eign person engaged in a long-term pattern or  
14 serious instances of conduct significantly ad-  
15 verse to the national security of the United  
16 States or the security and safety of United  
17 States persons; and

18 (B) any foreign country or foreign govern-  
19 ment identified as a strategic competitor in the  
20 National Defense Strategy issued by the Sec-  
21 retary of Defense on October 27, 2022.

22 (4) The term “covered foreign entity” means  
23 any business entity—

24 (A) that is subject, directly or indirectly  
25 through any chain of ownership, to the jurisdic-

1           tion, direction, or control of a covered foreign  
2           adversary; or

3           (B) in which any combination of entities  
4           subject, directly or indirectly through any chain  
5           of ownership, to the jurisdiction, direction, or  
6           control of a covered foreign adversary owns  
7           more than 20 percent of the outstanding voting  
8           stock or shares of the company.

9           (5) The term “covered port infrastructure  
10          equipment” means any operational technology,  
11          equipment, software, hardware, or cloud architecture  
12          in a covered strategic seaport that sends or receives  
13          any signal and is manufactured, controlled, or de-  
14          signed, in whole or in part, by a covered foreign en-  
15          tity.

16          (6) The term “covered strategic seaport” means  
17          a United States seaport—

18               (A) that is a strategic seaport, as such  
19               term is defined in section 3505(a) of the Na-  
20               tional Defense Authorization Act for Fiscal  
21               Year 2014 (Public Law 113–66; 46 USC 50302  
22               note); or

23               (B) that is determined by the Secretary of  
24               Homeland Security, in coordination with the  
25               Secretary of Defense, to be essential to the mili-

1           tary readiness, national security, and continuity  
2           of the economy of the United States.

3           (7) The term “significant event” means an  
4           event that causes severe degradation to economic ac-  
5           tivity in the United States and that is—

6                       (A) the result of a cyber attack; or

7                       (B) a natural disaster or human-caused se-  
8           curity incident.

